Branimation

Atif Mashkoor, Jean-Pierre Jacquot

BRANIMATION ⋆

Atif Mashkoor, Jean-Pierre Jacquot

LORIA – DEDALE Team – Nancy Université
Vandoeuvre-Lès-Nancy, France
{firstname.lastname}@loria.fr

1 The problem

Brama is one of animation tools for Event-B specifications supported by Rodin Platform. It enables quick validation of models. While animating an Event-B specification with Brama, sometimes we stumble upon some technical issues which prevent its execution. The situations where Brama cannot animate a specification can be arranged in a typology of five typical cases:

1 Brama does not support the finite clause in axioms
2 Brama must interpret quantifications as iterations
  2.1 Brama only operates on finite sets
  2.2 Brama cannot compute finite sets defined in comprehension with nested quantification
  2.3 Brama explicitly requires typing information of all those sets over which iteration is performed in an axiom
3 Brama cannot compute dynamic functional bindings in substitutions
  3.1 Brama does not support dynamic mapping of variables in substitutions
  3.2 Brama does not support dynamic function computation in substitutions
4 Brama does not compute functions defined analytically
  4.1 Functions with analytical definitions in context cannot be computed in events
  4.2 Functions using case analysis can not be expressed in a single event
  4.3 Invariants based on function computations can not be evaluated
5 Brama has limited communication with its external graphical animation environment

2 The solution

For each situation, we have defined a "heuristic" to transform the original specification into one that can be animated [1]. The heuristics are described following a rigid pattern as shown by fig 1.

We design the heuristics to preserve the behavior of the specification as specified by original model, and not its formal properties. So if some of the proof obligations can not be discharged, this is still acceptable.

⋆ This is a proposal for tool/plug-in development

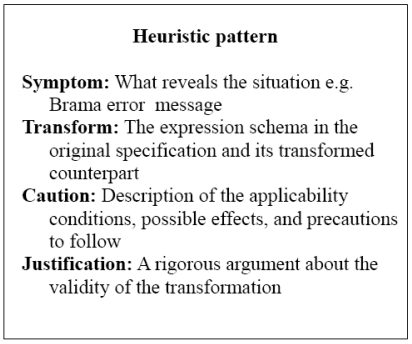

Fig. 1. The heuristic pattern

3 The observations

We experiment our heuristics on two case studies: a formal domain model of land transportation [2] and a situated multi-agent platooning system [3]. From these two experiences, we come to know that:

- Most well written specifications need to go through this transformational process in order to be animated correctly.
- Once heuristics are applied some of the proofs are impossible to discharge.
- We should not introduce these heuristics early during the specification phase before animation as they will further complicate the already complex text.
- It is a good idea to animate each refinement step like verification to gain confidence in your specification. Problems then can be detected and fixed right on the spot.

4 The need for tool

Though the proposed heuristics solve the aforementioned Brama problems, yet their manual application is tedious, cumbersome and may be error prone if not applied carefully. Therefore a plug-in/tool is required which can apply these transformations automatically to specifications. We don't want this tool to be highly intelligent or sophisticated, it can only performs basic functions, for example, removal of finite clause, provision of typing information, event replications, etc.

References

1. Mashkoor, A., Jacquot, J.P.: Incorporating Animation in Stepwise Development of Formal Specification. Research Report INRIA-00392996, LORIA, Nancy, France (2009)
2. Mashkoor, A., Jacquot, J.P., Souquières, J.: B événementiel pour la modélisation du domaine: application au transport. In: Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL'09), Toulouse, France (2009) 1–19
3. Lanoix, A.: Event-B specification of a situated multi-agent system: Study of a platoon of vehicles. In: 2nd IFIP/IEEE International Symposium on Theoretical Aspects of Software Engineering (TASE), IEEE Computer Society (2008) 297–304